УДК 004.032 **doi: 10.26906/SUNZ.2022.1.094**

С. І. Шаповалова, О. С. Гулак

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

БЛОКЧЕЙН ТЕХНОЛОГІЇ В БАНКІВСЬКІЙ СФЕРІ

Анотація. Предметом дослідження в статті є реалізація проведення банківських транзакцій. Мета роботи – представлення рішення з проведення банківських транзакцій на основі технології Блокчейн. В статті представлено базові системи переказу коштів між банками, надано спрощену схему проведення транзакції, а також програмну систему на її основі. Отримано наступні результати: надано рішення з програмної реалізації проведення транзакцій між банками на основі запиту клієнта. Висновки: 1) запропоновано схему проведення транзакцій з розрахункових операцій без банків-посередників; 2) на основі проведеного аналізу існуючих методів досягнення консенсусу обґрунтовано використання методу PoW та використання алгоритму хешування SHA256; 3) розроблено програмну реалізацію проведення фінансових транзакцій на основі технології Блокчейн, яка дозволяє проводити більш безпечні, швидкі та дешеві операції переведення коштів. Перспективним напрямком подальших досліджень є розширення можливих операцій з надання банківських послуг на основі технології Блокчейн.

Ключові слова: Блокчейн, розподілений консенсус, Proof-of-stake, Proof-of-work, банківські транзакції.

Вступ

На сьогоднішній день в банківських системах переведення коштів існує чимало недоліків. Насамперед це стосується забезпечення задовільного рівня безпеки цього процесу. Майже щодня особисті рахунки піддаються атакам хакерів. Крім цього для міжнародних переказів може знадобитися багато часу – до 3-7 банківських днів. Більшість переказів коштів потребують значних комісійних витрат, адже зазвичай грошові транзакції здійснюються через посередницьку структуру або організацію. Тому актуальним є вдосконалення програмного забезпечення проведення банківських операцій для підвищення безпеки та прискорення виконання транзакцій.

Постановка проблеми. Для переказу коштів між банками існує три базові системи.

1. Система відкладених нетто-розрахунків.

Більшість країн має подібну систему, наприклад, у Великобританії такою системою є BACS [1].

У таких системах на початковому етапі повідомлення (або файли) потрапляють у центральну «клірингову» систему, яка відстежує всі платежі і потім у визначені терміни розраховує нетто-суму, яку кожен із банків повинен будь-якому іншому банку.

На наступному етапі банки проводять між собою розрахункові операції безпосередньо або застосовують систему RTGS (Real-Time Gross Settlement) [2]. Валові розрахунки передбачають виконання кожного платежу в індивідуальному порядку, без використання нетто-схем, які використовують різницю між вхідними і вихідними грошовими потоками.

2. Система кореспондентських угод [3].

Така модель обробки платежів (і більш складних різновидів переказів) відома як діяльність банків з урахуванням кореспондентських відносин. Наявність кореспондентських відносин дозволяє банкам полегшити виплату платежів відповідним клієнтам.

3. Система платежів SWIFT [4].

Мережа SWIFT дозволяє банкам безперешкодно обмінюватися електронними повідомленнями. Один із типів повідомлень, який підтримується мережею SWIFT, – це MT103 [5]. MT103 надає можливість певному банку давати вказівки іншому банку, щоб останній перерахував суму на рахунок одного зі своїх клієнтів. У той час та сама сума списується з рахунку організації, що надсилає повідомлення. Тоді у банку, який приймає повідомлення, ця сума зараховується так, щоб усе врівноважувалося.

В кожній з існуючих систем присутні ризики контрагента, ліквідності та витрат. Найважливішою проблемою є забезпечення безпеки проведення транзакцій. Підвищити рівень безпеки можна завдяки використанню нових технологій обліку цифрових транзакцій в розподілених базах даних.

Технологія Блокчейн в значній мірі покладається на фундаментальні інструменти з криптології та безпеки даних, особливо з точки зору автентифікації транзакцій. Концепція Блокчейн унеможливлює несанкціонований доступ, тим самим підвищує стійкість до хакерських атак. У своїй найбільш абстрактній формі Блокчейн можна представити як захищену від зломів реєстраційну книгу, де зберігаються записи транзакцій між вузлами [6]. Замість реалізації централізованої системи баз даних за технологією Блокчейн база даних реплікується, тобто розподіляється по мережі та синхронізується через Інтернет.

Блокчейн називають головною технологічною інновацією, оскільки він містить інформацію про усі транзакції мережі [7]. Блокчейн-технологія наразі не реалізована в достатній мірі в фінансових системах. Однак Блокчейн має потенціал для розповсюдження у фінансовому та банківському секторі шляхом впровадження однорангової децентралізованої системи транзакцій.

Згідно з дослідженнями провідної світової консалтингової компанії Accenture [8], тільки в країнах західної Європи за рахунок впровадження Блокчейн банки можуть економити 8 мільярдів із загальної суми витрат у 30 мільярдів доларів в рік. Використання технології однорангового Блокчейн забезпечуватиме високий рівень безпеки виконання транзакцій.

Метою статті є представлення рішення з проведення банківських транзакцій на основі технології

Блокчейн. Для досягнення мети поставлено такі завдання:

1. Розробити схему проведення транзакцій на основі Блокчейн

2. Визначити методи хешування для задачі шифрування.

3. Розробити програмне забезпечення безпечного проведення фінансових транзакцій.

Методи реалізації

Блок — це одиниця Блокчейн, яка містить всі транзакції останнього сеансу або транзакції, обрані за заданим принципом. Після сеансу блок вбудовується в Блокчейн як елемент постійної бази даних.

Крім інформації про транзакції кожен блок містить посилання на попередній блок. Це посилання є розв'язком складної математичної задачі шифрування на основі необоротної криптографічної хеш-функції.

Для генерації цього посилання необхідно визначити випадкові числа, які в поєднанні з зашифрованим вмістом попереднього блоку генеруватимуть визначений результат. Комп'ютеру з 8 Гб оперативної пам'яті та 4-х ядерним процесором може знадобитись близько року на правильний підбір значень, але через велику кількість комп'ютерів в мережі, дана задача розв'язується в середньому в межах десяти хвилин.

Вміст кожного блоку представляється у зашифрованому вигляді як хеш. Хеш — це фрагмент даних фіксованої довжини, який можна асоціювати з відбитком пальця в кримінології. Хеші обчислюються за допомогою хеш-функцій. Перевага хешу полягає в тому, що якщо вхідні дані змінюються, вихідні дані також набуватимуть змін. Кожен блок в Блокчейн містить власний хеш, а також хеш попередника у своєму заголовку. Хеш повинен обчислюватися шляхом використання всієї інформації про блок. Метою його використання є захист цілісності даних блоку. Хеші широко використовуються в Блокчейн для представлення контрактів, маркерів, адрес гаманців. Навіть ідентифікатори транзакцій виражаються в хешах.

Хеші, які пов'язують кожен блок з його попередником, утворюють ланцюг до блоку генезису (першого блоку). Блок генезису є закодованим блоком, який не має посилання на попередній блок.

Технологія Блокчейн швидко розповсюджується в цифровому світі завдяки концепції, при якій кожна онлайн-транзакція, що виконана в минулому або ще виконується, може бути перевірена в будь-який час в майбутньому. Крім цього виконання транзакцій відбувається без завдання збитків конфіденційності цифрових активів залучених сторін. Важливими перевагами технології Блокчейн є анонімність та розподілений консенсус (Distributed Consensus). Для реалізації останнього у розподіленій базі даних задіяно відповідний механізм консенсусу.

Механізм консенсусу - це метод узгодження вузлами комп'ютерної мережі значення запропонованої транзакції або частини її даних, які в майбутньому будуть додані до Блокчейн у якості нових блоків.

Існує два основних методи досягнення консенсусу: PoS (Proof-of-stake) та PoW (Proof-of-work) [9]. В обох методах використовується поняття блоку.

Метод PoW запропоновано на початку 1990-х років [10]. Схема методу PoW містить такі етапи:

1. Створення блоку.
2. Розв'язання задачі генерації посилання блоку. Перевірка законності транзакції здійснюється всередині кожного блоку. Найперше вирішення задачі отримує винагороду. Таким чином стимулюється виконання складних перевірок. Винагорода виплачується як комісія з транзакції.
3. «Вбудова» поточного блоку в Блокчейн.

Після перевірки транзакції «вбудовуються» в загальнодоступний Блокчейн. Цей процес називають майнінгом (mining). Особливостями методу PoW є:

1. Необхідність виконання задачі, яка потребує багато обчислювальних ресурсів;
2. Можливість легкої та швидкої перевірки отриманого результату.

Метод PoS [11], представлений в 2012 році, є модифікацією PoW. На відміну від Блокчейн-систем на основі PoW методів, Блокчейн PoS не визначають автора блоків, виходячи виключно з наявної обчислювальної потужності та можливостей споживання енергії. Цей метод використовує випадково обрані валідатори (майнери) для перевірки блоків транзакцій. Крім цього, вимагається надання певної кількості криптовалюти в якості застави, що називається стейкингом (staking). Оскільки в методі PoS автори блоків невідомі, його небезпечно використовувати для реалізації банківських транзакцій. Тому для розробки запропонованої системи було обрано метод PoW для виконання операцій над хеш-функціями. Для досягнення розподіленого консенсусу обрано хеш-функцію SHA256.

Реалізація банківських транзакцій

В загальному вигляді схема розрахунків та відповідні системи їх забезпечення представлено на рис. 1.

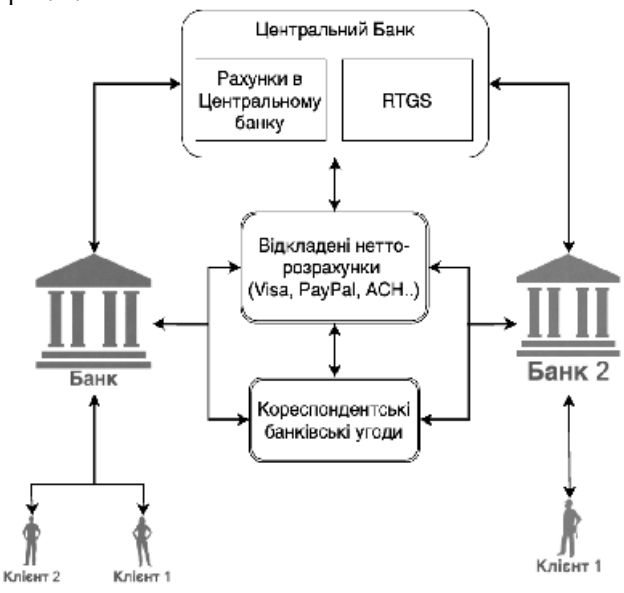

Рис. 1. Схема взаємодії клієнтів різних банків

Схема взаємодії клієнтів банків на рис. 1 відображає вищезазначені базові системи переказу коштів, окрім SWIFT.

Завдяки технології Блокчейн з'являється можливість здійснювати фінансові операції децентралізованим способом без залучення третіх сторін або центральних органів для цілей ведення обліку.

Відповідна схема представлена на рис. 2.

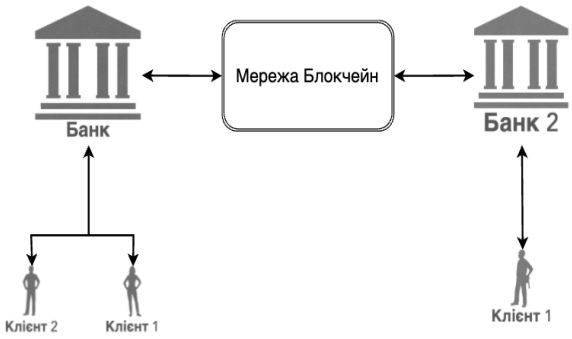

Рис. 2. Схема проведення транзакцій в системі на основі Блокчейн

Фактично всі системи, які забезпечують посередництво можна замінити мережею Блокчейн. Ця мережа складається з блоків представлення транзакцій. Таким чином розрахунки між банками проводяться без посередників та відкладення операцій та перевірок. Сеанс передачі коштів (виконання транзакцій) між двома клієнтами здійснюється за алгоритмом, представленим на рис. 3.

Програмна система забезпечує користувачу можливість створення транзакцій для переведення коштів в будь-якій валюті на гаманець іншого користувача, що дозволяє оминути весь процес переведення коштів через системи SWIFT, міжнародні банки, уникати величезних комісій та довгих очікувань проходження транзакції.

Таким чином технологія Блокчейн дозволяє подолати недоліки централізованої банківської системи, де користувачу доводиться залежати від третьої сторони для здійснення операцій.

Розроблена система має модульну реалізацію. Система містить такі основні модулі (рис. 4):

- Блокчейн;
- API (Бекенд частина);
- Мобільний застосунок.

В модулі Блокчейн вирішуються такі задачі:

1. Генерація та розсилка запиту на розв'язання задачі генерації посилання блоку.
2. Побудова блоку на основі отриманого хешу з розв'язком задачі.
3. Організація доступу для переведення коштів на основі запитів API модуля.

Перевірка гаманців відправника та отримувача коштів.

При успішному виконанні надісланих запитів дані транзакції генеруються і закодовуються в блок, в який додається посилання на попередній блок вузла блокчейну.

За допомогою мобільного застосунку користувач створює транзакцію:

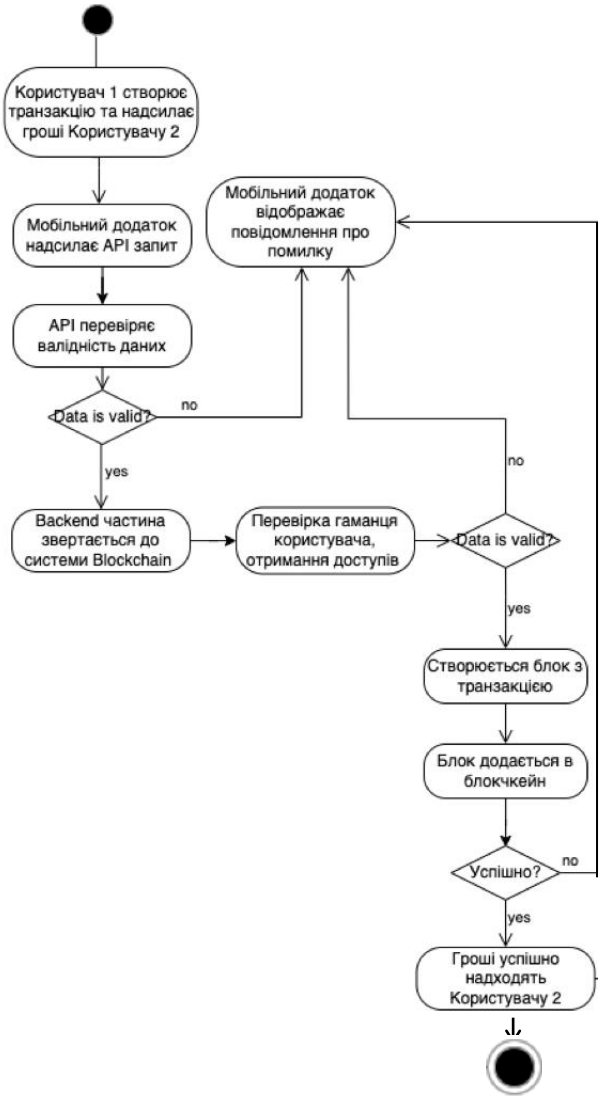

Рис. 3. Виконання транзакції з передачі коштів

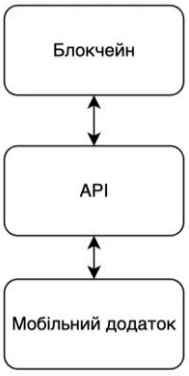

Рис. 4. Схема взаємозв'язків модулів системи

1. Вносить основні дані, такі як адреса гаманця отримувача, валюта переведення коштів, потрібна сума переведення.
2. Обирає гаманець, з якого будуть надіслані кошти.

Після заповнення даних транзакції мобільний застосунок надсилає запит на бекенд частину системи, де одразу перевіряється валідність введених даних та вживаються відповідні заходи. У випадку

невалідних даних - у відповідь в додаток користувачу надходить код та повідомлення помилки. У випадку успішної валідації вхідних даних - бекенд звертається до модуля Блокчейн.

В API реалізовано програмне забезпечення зв'язку з вузлами комп'ютерної мережі. Для цього використано Websockets API та HTTP-запити.

Запропонована система надає користувачам графічний інтерфейс для проведення транзакцій та функціонал обміну даними, представленими у вигляді ланцюжку блоків. Також система забезпечує майнінг і обмін валюти. Таким чином, користувачам забезпечується можливість безпечного здійснення будь-яких грошових операцій. Така методологія передбачає значне скорочення витрат коштів на комісії та надає можливість уникнути вразливостей, пов'язаних з безпекою.

Міцність безпеки Блокчейн постійно збільшується в геометричній прогресії і все більше блоків видобувається та зберігається в мережі, що робить практично неможливим змінення транзакції.

Запропонована система проведення банківських транзакцій має такі переваги:

1. Підвищується рівень безпеки проведення транзакцій.
2. Пришвидшуються розрахункові операції.
3. Значно зменшуються комісійні витрати.

Висновки

1. Запропоновано схему проведення транзакцій з розрахункових операцій без банків-посередників.

2. На основі проведеного аналізу існуючих методів досягнення консенсусу обґрунтовано використання методу PoW та використання алгоритму хешування SHA256.

3. Розроблено програмну реалізацію проведення фінансових транзакцій На основі технології Блокчейн, яка дозволяє проводити більш безпечні, швидкі та дешеві операції переведення коштів.

Перспективним напрямком подальших досліджень є розширення можливих операцій з надання банківських послуг на основі технології Блокчейн.

СПИСОК ЛІТЕРАТУРИ

1. BACS About Technical Resources [Electronic resource] // Schneider Electric – Access mode: https://www.bacs.co.uk/About/Pages/About.aspx.
2. A brief introduction to RTGS and CHAPS // 2021 – С. 122-138.
3. Івасів Б.С. Міжнародні розрахунки та валютні операції / Б.С. Івасів, Л.М. Прийдун, В.Я. Рудан // Навчальний посібник, 2013, № 1. – С. 40–53
4. Міжнародна система S.W.I.F.T. [Electronic resource] // Schneider Electric – Access mode: https://www.bacs.co.uk/About/Pages/About.aspx.
5. Greater visibility and transparency over your international payments [Електронний ресурс] // Schneider Electric – Режим доступу до ресурсу: https://www.moneymover.com/about/faqs/what-mt103/.
6. Crosby M. Blockchain Technology / Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. // Berkeley Education, Sutardja Center for Entrepreneurship & Technology Technical.
7. Dr. Lata Ragha. Blockchain Technology in Financial and Banking Sector / Dr. Lata Ragha, Ameya Dixit, Blaze Rodrigues, Kaustubh Yadav, Thomas Chacko // International Journal of Trend in Research and Development. – 2018. – №1. – P. 41–44.
8. Banking on blockchain. A value analysis for investment banks [Electronic resource]/ Schneider Electric – Access mode: https://www.accenture.com/t20170120t074124z__w__/us-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/consulting/accenture-banking-on-blockchain.pdf.
9. Fukumits M. A Proposal of a Secure P2P-type Storage Scheme by using the Secret Sharing and the Blockchain / Masayuki Fukumits, Shingo Hasegawa, Jun-yaIwazaki, Masao Sakai, Daiki Takahashi. // IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), 2017.
10. Dwork C. Pricing via Processing Or Combatting Junk Mail, Advances in Cryptology / Cynthia Dwork, Moni Naor. // CRYPTO 1992. Annual International Cryptography Conference, 1992.
11. What Is Proof of Stake (PoS) in Crypto? [Electronic resource] // Schneider Electric – Access mode: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-stake/.

Received (Надійшла) 18.01.2022
Accepted for publication (Прийнята до друку) 16.03.2022

Blockchain technology in banking

S. Shapovalova, O. Hulak

Abstract. The subject of research in the article is the implementation of banking transactions. The purpose of the work is to present a solution for conducting banking transactions based on Blockchain technology. The article presents the basic systems for transferring funds between banks, provides a simplified scheme for conducting a transaction, as well as a software system based on it. The following results were obtained: a solution for the software implementation of transactions between banks based on a client's request is presented. Conclusions: 1) a scheme for conducting transactions on settlement operations without intermediary banks is proposed; 2) based on the analysis of existing methods for reaching consensus, the use of the PoW method and the use of the SHA256 hashing algorithm are justified; 3) a software implementation of financial transactions based on Blockchain technology has been developed, which allows for safer, faster and cheaper fund transfer operations. A promising direction for further research is the expansion of possible operations for the provision of banking services based on Blockchain technology.

Keywords: Blockchain, distributed consensus, Proof-of-Stake, Proof-of-Work, banking transaction.